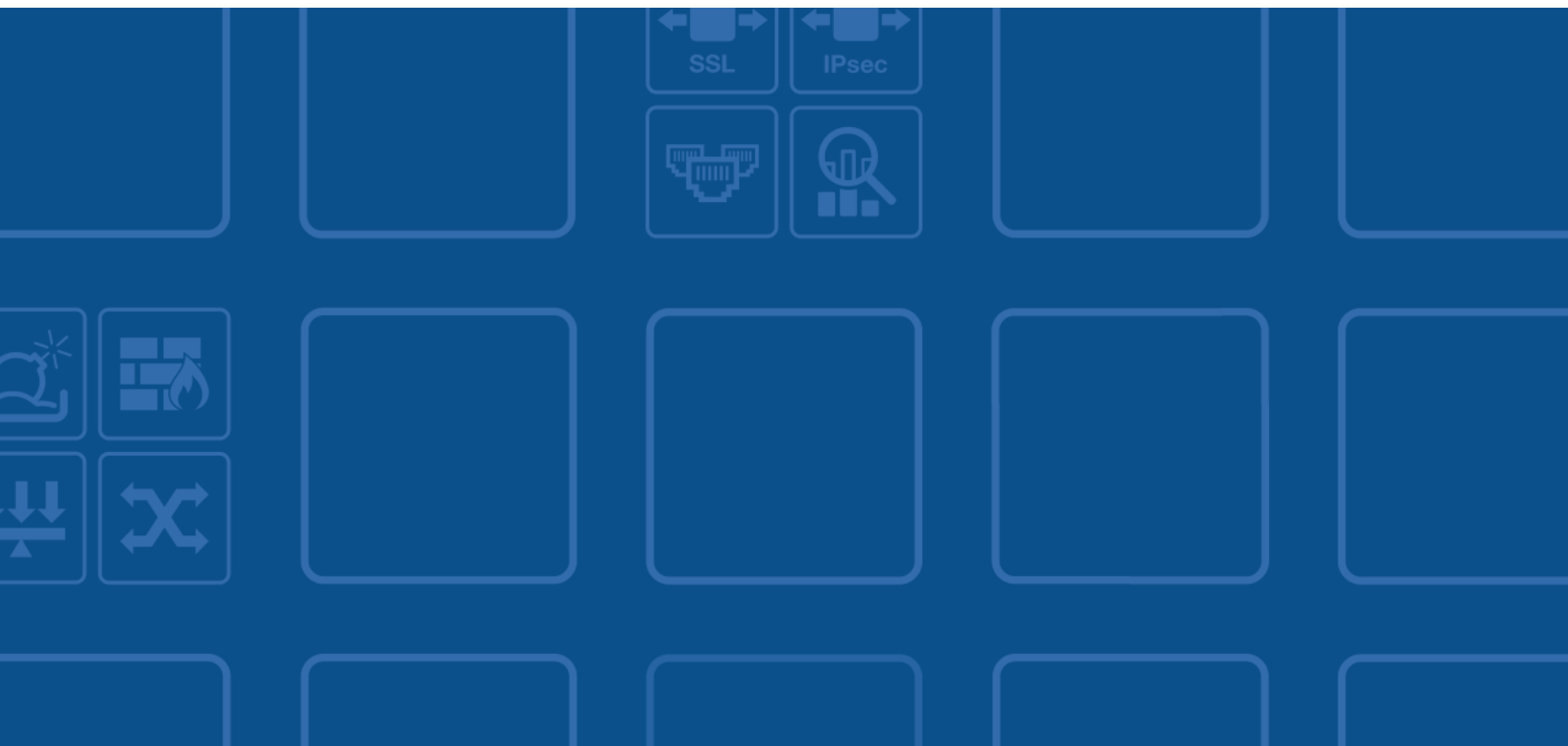
FORTINET
High Performance Network Security

# FortiClient EMS for Chromebooks - Administration Guide

VERSION 1.0.5



**FORTINET DOCUMENT LIBRARY**

http://docs.fortinet.com

**FORTINET VIDEO GUIDE**

http://video.fortinet.com

**FORTINET BLOG**

https://blog.fortinet.com

**CUSTOMER SERVICE & SUPPORT**

https://support.fortinet.com

**FORTIGATE COOKBOOK**

http://cookbook.fortinet.com

**FORTINET TRAINING SERVICES**

http://www.fortinet.com/training

**FORTIGUARD CENTER**

http://www.fortiguard.com

**END USER LICENSE AGREEMENT**

http://www.fortinet.com/doc/legal/EULA.pdf

**FEEDBACK**

Email: techdocs@fortinet.com

June 13, 2017

FortiClient EMS for Chromebooks 1.0.5 Administration Guide

04-105-372713-20170613

# TABLE OF CONTENTS

# Change Log

| Date | Change Description |
| --- | --- |
| 2017-03-30 | Initial release |
| 2017-05-16 | Updated information about SSL certificates. |
| 2017-06-13 | Updated information about creating unique service account credentials. |

# Introduction

FortiClient Enterprise Management Server - Chromebook (FortiClient EMS for Chromebooks) is a security management solution that works with FortiClient to provide web filtering for Google Chromebooks.

FortiClient EMS for Chromebooks is designed to meet the needs of small to large enterprises that deploy FortiClient on Google Chromebooks. Some of the benefits of deploying FortiClient EMS for Chromebooks include:

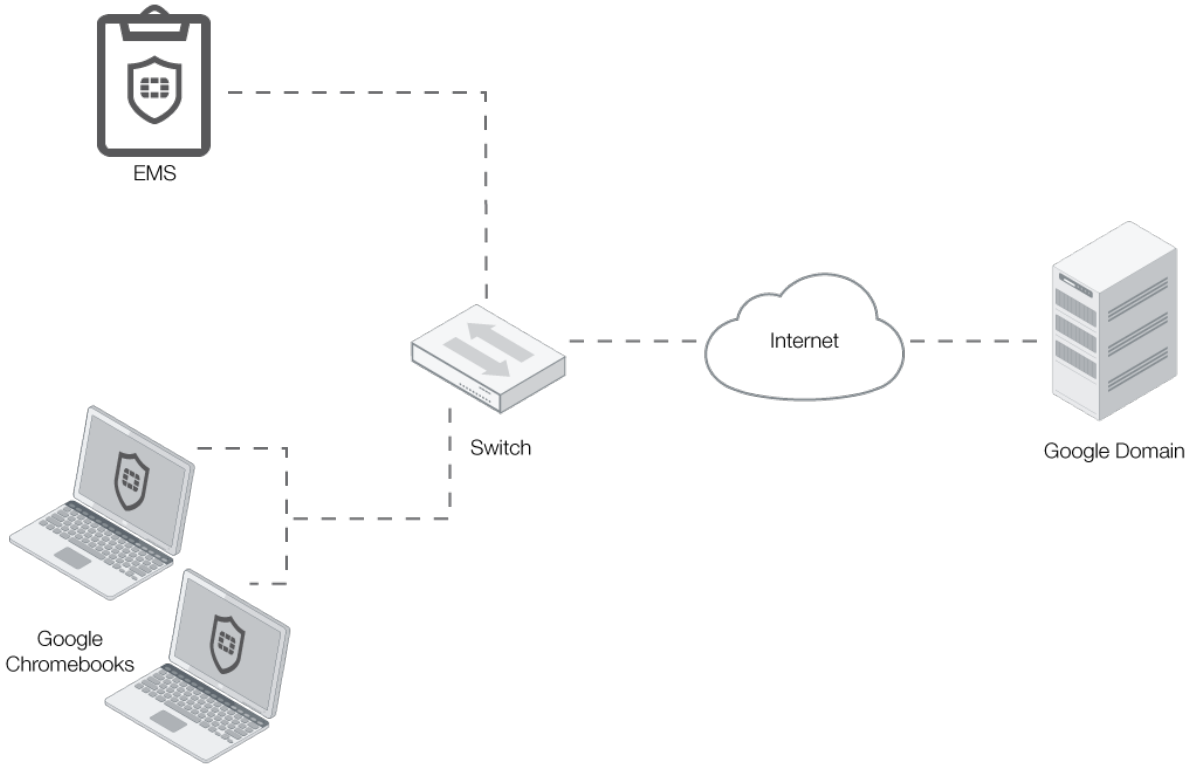
- Defining web filtering rules in a profile and remotely deploying the profile to FortiClient on Google Chromebook endpoints
- Updating profiles for users of Google chromebook regardless of access location
- Monitoring Google Chromebook endpoints

## Components of FortiClient EMS for Chromebooks

FortiClient EMS for Chromebooks provides the infrastructure to install and manage the FortiClient Web Filter extension on Google Chromebook endpoints. FortiClient protects endpoint users by working with FortiClient EMS for Chromebooks to filter the web content that endpoint users can view on Google Chromebook.

The following table lists the components of FortiClient EMS for Chromebooks.

| Component | Description |
|---|---|
| **FortiClient EMS for Chromebooks** | Manages web filtering on Google Chromebook endpoints with the FortiClient Web Filter extension installed that connect to your Google Domain. It includes the following software:<br>• The console software that manages security profiles and Chromebook endpoints.<br>• The server software provides secure communication to and from the Chromebook endpoints and the Google Admin console. |
| **Database** | Stores security profiles, events, and user information retrieved from the Google Admin console. The SQL database is installed as part of the FortiClient EMS installation. |
| **FortiClient Web Filter extension** | Communicates with FortiClient EMS for Chromebooks and enforces web filtering on Google Chromebook endpoints. |




FortiClient EMS for Chromebooks allows you to:

- Establish and enforce security profiles
- Manage security profiles from an integrated management console
- Obtain a consolidated view of multiple security profiles across all endpoints in your Google Domain
- Monitor endpoints' web browsing activity

## FortiClient EMS and Fortinet Endpoint Security Management

FortiClient EMS for Chromebooks is part of the Fortinet Endpoint Security Management suite, which ensures a comprehensive policy administration and enforcement for an enterprise network.

## Documentation

You can access the FortiClient EMS for Chromebooks documentation from the following link: docs.fortinet.com

The FortiClient EMS for Chromebooks documentation set includes the following documents:

- *FortiClient EMS for Chromebooks 1.0.5 Release Notes*
  This document describes new features and enhancements in the FortiClient EMS for Chromebooks system for the release and lists any known issues and limitations. This document also defines supported platforms and the required minimum system requirements.

- *FortiClient EMS for Chromebooks 1.0.5 QuickStart Guide*

  This document describes how to install and begin working with the FortiClient EMS for Chromebooks system. It provides instructions on installation, deployment, and also includes a high-level task flow for using the FortiClient EMS for Chromebooks system.

- *FortiClient EMS for Chromebooks 1.0.5 Administration Guide*

  This document describes how to set up FortiClient EMS for Chromebooks and use it to manage FortiClient endpoints. It includes information on how to configure multiple endpoints, configure and manage profiles for the endpoints, and view and monitor the FortiClient endpoint profile status.

# What's New

The new features in FortiClient EMS for Chromebooks 1.0.5 include the following:

## FortiClient EMS for Chromebooks 1.0.4

There are no new features or enhancements for FortiClient EMS for Chromebooks 1.0.4.

## FortiClient EMS for Chromebooks 1.0.3

There are no new features or enhancements for FortiClient EMS for Chromebooks 1.0.3.

## FortiClient EMS for Chromebooks 1.0.2

### Google Domain management

FortiClient EMS for Chromebooks is integrated with Google Domain. The administrator may manage users in EMS by importing them from Google Domain. The full domain or any organizational unit (sub-OU) can be imported. FortiClient profiles may be assigned to, or unassigned from, the OU. If no longer required, Google Domain may be deleted from EMS.

If there are changes in Google Domain records, EMS will automatically update the imported data, adjusting the OU as appropriate.

### FortiClient web filtering feature

The EMS administrator will configure the Chromebook via the Google Domain Admin console. When any of the users in the domain log in to their Chromebook with their Google Domain account, FortiClient will be installed on their Chromebook.

FortiClient provides web filtering on each Chromebook. Following installation, it will retrieve a profile from the EMS. The profile is appropriate to the logged-in user. It is applied to each web page request from the Chromebook. If the user attempts to access a prohibited or blocked page, access will be denied, and a replacement message will be displayed in the web browser.

### FortiClient EMS - Chromebook profile management

FortiClient EMS provides web filtering profiles. Each profile defines the FortiGuard categories to be blocked, allowed or monitored on the Chromebook. EMS administrator may create, modify, assign, unassign or delete profiles. FortiClient on the Chromebook will download the profile assigned based on the logged-in user.

Web Filtering profile may include exclusion lists, which consists of blacklists and whitelists. Safe search is also provided for the main search engines – Google, Yahoo!, and Bing safe search for text.

EMS administrator may also configure to upload logs to FortiAnalyzer. When configured, Chromebooks will send logs to the configured FortiAnalyzer.

## FortiClient EMS - Chromebook dashboard

FortiClient EMS - Chromebook dashboard can display the real-time status of Chromebooks, including how many users are managed or unmanaged, and how many users are in active or inactive state. It can also display the Web Filter Violation summary and users with a Web Filter Violation summary. It also allows the EMS admin to drill down to the detailed information view for the Web Filter violation or users with violations from the selected pie chart.

The EMS admin can also import and upgrade the EMS license from the dashboard.

## FortiClient EMS - Chromebook user management

Default admin or configured super-administrator of the FortiClient EMS - Chromebook Server can manage Chromebook users. Default admin or configured super-administrator is allowed to configure the default EMS admin user's password. They can also add or remove the EMS administrator, and configure various EMS server permissions for them.

## Detail information view for Google Domain users

FortiClient EMS - Chromebook Server provides a detailed information view for each managed Chromebook user. It reports the Google user's profile name and displays the client statistics for blocked site distribution and all sites distribution. The detailed Client view also provides the list of all blocked site logs for the selected Chromebook user.

## Log upload to FortiAnalyzer

If the EMS administrator configures to upload logs to FortiAnalyzer, Chromebooks will send all FortiClient logs to the configured FortiAnalyzer. If the FortiAnalyzer is not accessible, FortiClient will keep the log in the local storage until FortiAnalyzer becomes accessible. Then, it will start to send the old logs and new logs to FortiAnalyzer.

# Overview

This section provides an overview of how to:

- Install and configure FortiClient EMS for Chromebooks.
- Configure Google Admin console
- Deploy profiles to Chromebooks
- Monitoring Chromebooks and updating profiles

This section also includes a description of how FortiClient EMS for Chromebooks and FortiClient work with Google Chromebooks after the setup is complete.

## Installing and configuring FortiClient EMS for Chromebooks

Before installing FortiClient EMS for Chromebooks, it is recommended that you read the *FortiClient EMS - Chromebook Release Notes* available on docs.fortinet.com to become familiar with relevant software components and other important information about the product.

Following is an overview of how to install and configure FortiClient EMS for Chromebooks.

1. Prepare for the FortiClient EMS installation. See Requirements and Dependencies on page 15.
2. Download and install FortiClient EMS. See Installing FortiClient EMS for Chromebooks on page 20.
3. Log into FortiClient EMS. See Logging into FortiClient EMS on page 21.
4. License FortiClient EMS. See Licenses on page 18.
5. Add unique service account credentials. See Configuring unique service account credentials on page 32.
6. Add SSL certificates. See Adding SSL certificates on page 40.
7. Configure FortiClient EMS for Chromebooks settings. See Settings on page 40.
8. Configure user accounts and permissions. See User Management on page 45.

## Configuring the Google Admin console

Following is an overview of how to configure the Google Admin console to prepare for adding the Google domain to FortiClient EMS for Chromebooks. The document assumes that you have created the Google domain.

1. Log into the Google Admin console. See Logging into FortiClient EMS on page 21.
2. Add the FortiClient Web Filter extension. See Adding the FortiClient Web Filter extension on page 23.
3. Configure the FortiClient Web Filter extension. See Configuring the FortiClient Web Filter extension on page 24.
4. Add root certificates. See Adding root certificates on page 25.
5. Add service account credentials. See Logging in to the Google Admin console on page 23.
6. Disallow incognito mode. See Disallowing incognito mode on page 27.

## Deploying profiles to Chromebooks

Following is an overview of how to add a Google domain, configure profiles, and push profiles to Google Chromebooks.

After you add the extension in Google Admin console, the extension is downloaded to the Google Chromebook when the Chromebook user logs onto Chromebook.

1. Add the Google domain. See Adding Google domains on page 48.
2. Define web filtering options in one or more profiles. See Adding new profiles on page 52.
   You can enable Safe Search in profiles.
3. Assign profiles to domains to deploy profiles to FortiClient on endpoints. See Pushing profile changes to Google Chromebooks on page 54.
4. Verify the FortiClient Web Filtering extension. See Verifying the FortiClient Web Filtering extension on page 30.

## Monitoring Chromebooks and updating profiles

**To monitor Chromebooks:**

1. Click one of the Google domains in EMS and all the users in the domain will be listed.
2. Click one of the users, the user details, statistics and logs for that user will be displayed.
3. Click one of the pie charts in the dashboard.

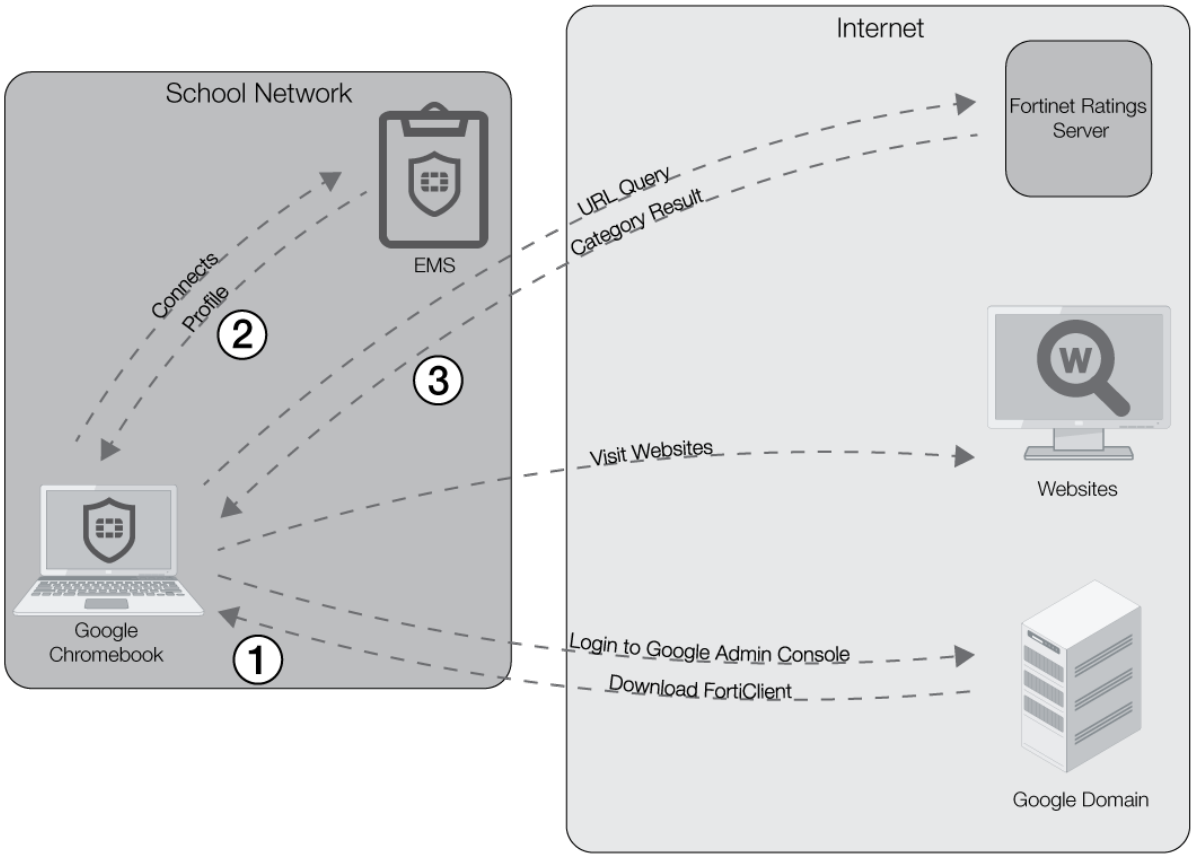
**To update profiles:**

1. Assign a new profile. See Assigning profiles to Google Chromebooks on page 54.
2. Edit profiles. See Editing profiles on page 54.

## How FortiClient EMS for Chromebooks and FortiClient work with Chromebooks

After you install and configure FortiClient EMS for Chromebooks, the Google Admin console, and the FortiClient Web Filter extension, the products work together to provide web-filtering security for Google Chromebooks that are logged into the Google domain. Following is a summary of how the products work together after the setup is complete:

1. When Google Chromebook users log into Chromebook, Google Chromebook downloads the FortiClient Web Filter extension.
2. FortiClient connects to FortiClient EMS for Chromebooks, and downloads a profile to Google Chromebook. The profile contains the web-filtering settings from FortiClient EMS.
3. When Google Chromebook users browse the Internet, FortiClient sends the URL query to the Fortinet Ratings server, and the Fortinet Ratings server returns the category result to FortiClient. FortiClient compares the category results with the profile to determine whether to allow the Google Chromebook user to access the URL.


Internet
School Network
Fortinet Ratings Server
EMS
URL Query
Category Result
Connects
Profile
2
3
Visit Websites
Websites
Google Chromebook
1
Login to Google Admin Console
Download FortiClient
Google Domain

# Requirements and Dependencies

You can install and use FortiClient EMS for Chromebooks as a standalone product on an active directory server or a standalone Windows machine. Requirements for installation and operation vary in relation to the presence of other software on the server and according to how you use FortiClient EMS for Chromebooks.

## Required services and ports

You must ensure that required ports and services are enabled for use by FortiClient EMS for Chromebooks and its associated applications on your server. The required ports and services enable FortiClient EMS for Chromebooks to communicate with clients and servers running associated applications.

| Communication | Service | Protocol | Port |
|---|---|---|---|
| **Apache** | HTTPS | TCP | 443 |
| **SQL server** | | | |
| **FortiClient on Chrome OS**<br>• Connection to Profile Server. | | | 8443 (default)<br>You can customize this port. |

## Management capacity

FortiClient EMS for Chromebooks is intended for use by enterprises. It has the capacity to manage a large number of endpoints. The following are suggested EMS host system hardware configurations, depending on the number of endpoints being managed.

**Suggested minimum EMS system hardware**

You will need at least **200GB** of free disk space available.

| Max number of managed endpoints | Number of virtual CPUs | Memory (RAM) (in GB) | Suggested keep alive interval |
|---|---|---|---|
| 10, 000 | 2 | 8 | default |
| 20, 000 | 4 | 8 | default |
| 30, 000 | 4 | 8 | 120 seconds |

| Max number of managed endpoints | Number of virtual CPUs | Memory (RAM) (in GB) | Suggested keep alive interval |
|---|---|---|---|
| 40, 000 | 4 | 8 | 120 seconds |
| 50, 000 | 4 | 8 | 120 seconds |
| **Suggested minimum EMS system hardware** | | | |
| 75, 000 | 8 | 16 | 120 seconds |

For the purpose of this table, an Intel i5 processor with two cores and two threads per core will be considered to have 4 virtual CPUs. An Intel i3 processor with two cores and one thread per core has two virtual CPUs.

## Server readiness checklist for installation

Use the following checklist to prepare your server for installation.

| Checklist | Readiness Factor |
|---|---|
| | Temporarily disable security applications. You must temporarily disable any antivirus software on the target server before you install FortiClient EMS. Installation might be slow or disrupted while these programs are active. Note that a server might be vulnerable to attack when you uninstall or disable security applications. |
| | It is recommended to sync the time to the Google server time. |
| | Confirm that required services and ports are enabled and available for use by FortiClient EMS. |
| | Ensure that no conflict exists with Port 443 for Apache service to function properly. |

## Google for Work account

You will need to sign up for your own *Google For Work* account before you can use the Google service and manage your Chromebook users.

The *Google for Work* account is different from the free consumer account. The *Google for Work* account is a paid account that gives you access to a range of Google tools, services and technology.

You can sign up for a Google for Work account here: https://www.google.com/a/signup/#0

In the sign up process, you will need to use your email address to verify your Google Domain. This is also to prove that you have ownership of the domain.

# SSL certificates

FortiClient EMS for Chromebooks requires an SSL certificate signed by a Certificate Authority (CA) in pfx format. Use your CA to generate a certificate file in pfx format, and remember the configured password. For example, the certificate filename is *server.pfx* with password 111111.

The server where FortiClient EMS for Chromebooks is installed should have an FQDN (fully qualified domain name), such as ems.forticlient.com, and you must specify the FQDN in your SSL certificate.

If you're using a public SSL certificate, the FQDN can be included in either *Common Name* or *Subject Alternative Name*. You must add the SSL certificate to FortiClient EMS for Chromebooks. See Adding SSL certificates on page 40. You do not need to add the root certificate to Google Admin console.

If you're using a self-signed certificate (non-public SSL certificate), the *Subject Alternative Name* of your certificate must include DNS:<FQDN>, for example, DNS:ems.forticlient.com. You must add the SSL certificate to FortiClient EMS for Chromebooks, and you must add the root certificate to Google Admin console to allow the extension to trust FortiClient EMS for Chromebooks. See Adding root certificates on page 25.

# Licenses

This section describes the licensing options available for FortiClient EMS for Chromebooks. It provides information about the number of supported Google Chromebooks for each type of license to help you determine which license best suits your needs.

## Description of licenses for FortiClient EMS

FortiClient EMS for Chromebooks supports the following types of licenses:

- Free trial license
- Purchased license

### Free trial license

When you install FortiClient EMS for Chromebooks, the free trial license is enabled by default. The free trial license supports 10 Google Chromebook users. FortiClient EMS for Chromebooks consumes one license count for each managed Google Chromebook.

### Purchased license

Each purchased license allows management of one Google Chromebook user. You will need to purchase a minimum of 100 Google Chromebook users and you have an option to have this EMS license for a maximum three year term. You can specify the number of Google Chromebook users and the duration of term at the time of purchase.

## Licensing FortiClient EMS

The following will describe how to license FortiClient EMS.

1. Visit forti.net/Reseller to find a Reseller.
   Once you purchase FortiClient EMS, you will receive the *FortiClient Host Security License Certificate* via email. This email contains the *Certificate Number* that will be used to obtain the FortiClient EMS License.
2. Login to the Fortinet Support site.
   a. Click *Register and Renew*.
   b. Enter the *Certificate Number*. This is the number you received in the FortiClient Host Security License Certificate email.
      If you have not already registered an EMS device, you will be prompted to do so. This will require obtaining the *Hardware ID* from FortiClient EMS. You can obtain the *Hardware ID* by clicking the *Upgrade* link located in the *FortiClient EMS Dashboard*.
   c. Enter the *Hardware ID*.

d. Enter the *Fortinet Partner Reseller*.
e. Read, verify and agree to the *Terms and Conditions* of the service.
f. Verify the Product Entitlement List for your recent FortiClient EMS purchase. Check the *By accepting these terms...* checkbox. Then, click *Confirm*. The license file will now be available to use with your FortiClient EMS installation.
g. Click *Finish*.
h. From your *Products List*, select FortiClient EMS.
i. From the left panel, select *License and Key*.
j. From the *Available Keys List*, select the FortiClient EMS entry. Then, click *Get the License File*.
k. From FortiClient *EMS Dashboard* > *Upgrade*, click *Browse*.
l. Select the license file and *Upload File*. You have successfully licensed FortiClient EMS.

If you need to renew your license or make changes to your requirements, please contact Fortinet Support.

An instructional video on how to obtain licensing for FortiClient EMS is available in the Fortinet Video Library.

## Upgrading the FortiClient EMS license

**To upgrade the FortiClient EMS license:**

1. Go to *View* > *Upgrade License*. The *Add FortiClient EMS License* pane is displayed.
2. Click *Browse*, locate the license key file, and click *Upload File*.

## Licenses for component applications

Common services or applications do not require a license. See the *FortiClient Enterprise Management Server - QuickStart Guide* for more information about the common components.

During the installation of common services required for FortiClient EMS, you are not asked for license information.

## Help with licensing

For licensing issues with FortiClient EMS, contact the licensing team at Fortinet Technical Assistance Center (TAC):

- Phone: +1-866-648-4638
- Technical support: support.fortinet.com/

# Installation

Before you install and license FortiClient EMS for Chromebooks on a server, ensure you have:

- Reviewed Description of licenses for FortiClient EMS on page 18
- Met the requirements listed in the Requirements and Dependencies on page 15
- Completed the Server readiness checklist for installation on page 16
- Logged into the server as administrator. The administrator user account is equivalent to a Windows administrator account and provides access to all common services, FortiClient EMS, and other application tasks. You can use this account to initially log in to the server and to create other user accounts for normal day-to-day use of the applications.

It is recommended that you install FortiClient EMS for Chromebooks on a dedicated server in a controlled environment. Installing other software applications can interfere with the normal operation of FortiClient EMS for Chromebooks.

## Installing FortiClient EMS for Chromebooks

Installing FortiClient EMS for Chromebooks requires the following steps:

1. Be aware of software dependencies.
2. Download FortiClient EMS for Chromebooks.
3. Install FortiClient EMS for Chromebooks.

### Downloading FortiClient EMS for Chromebooks

You can download the FortiClient EMS for Chromebooks installation program from Fortinet Support.

Download the following `.exe` file: `FortiClientEnterpriseManagement_Chromebook_1.0.5.0130_x64.exe`

### Installing FortiClient EMS for Chromebooks

**To install FortiClient EMS for Chromebooks:**

1. Double-click the downloaded installation file for FortiClient EMS for Chromebooks. The installation wizard starts.

If you are not logged into the server as an administrator, right-click the installation file and select *Run as administrator*.

2. Follow the installation wizard instructions.
   In the License terms and agreement window: Select *I agree to the license terms and conditions* if you agree with the license terms and conditions. If you do not agree, the installation process stops.
3. Click *Install*.

The applications that will be installed appear. The FortiClient EMS installation package includes the following applications: *FortiClient EMS, Microsoft SQL Server 2014 Express Edition, Apache HTTP server, and Python*. The installation setup process begins.

4. Continue following the installation wizard instructions.
   After the program has installed, the *Setup Successful* window appears.
5. Click *Close*.
   A desktop icon is created, which opens the FortiClient EMS application home page.
6. Re-enable any antivirus applications that you temporarily disabled.

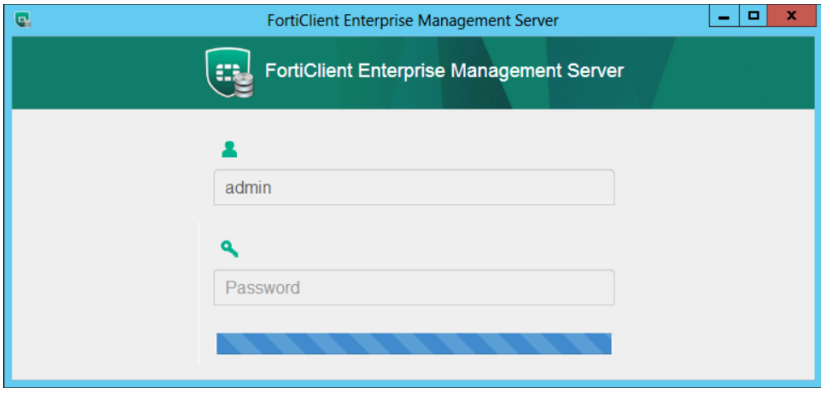
FortiClient EMS Server 1.0.5 does not support customized installation.

## Logging into FortiClient EMS

FortiClient EMS runs as a service on Windows computers.

**To open FortiClient EMS:**

1. Double-click the FortiClient EMS icon, or select *Start* > *All Programs* > *FortiClient Enterprise Management Server* to start the application.
2. Log in by using the default admin account. Enter `admin` for user name, and leave the password field empty. Click *Sign in*. The FortiClient EMS application opens.




The client automatically closes if it is idle for 30 minutes.

3. Add a password to the administrator account by going to *View* > *User Management*. See also Configuring User Management on page 45.
4. To exit the application, click *Admin* > *Logout* from the toolbar.

# Uninstalling FortiClient EMS

Use the *Programs and Features* pane of the Control Panel in Microsoft Windows to uninstall FortiClient EMS for Chromebooks.

FortiClient EMS for Chromebooks installs the following dependencies. If they are not being used by other applications on the same computer, they can be uninstalled manually after the EMS has been removed.

- Microsoft ODBC Driver 11 for SQL Server
- Microsoft SQL Server 2008 Setup Support Files
- Microsoft SQL Server 2012 Native Client
- Microsoft SQL Server 2014 (64-bit)
- Microsoft SQL Server 2014 Setup (English)
- Microsoft SQL Server 2014 Transact-SQL ScriptDom
- Microsoft Visual C++ 2010 x64 Redistributable – 10.0
- Microsoft Visual C++ 2010 x86 Redistributable – 10.0
- Microsoft Visual C++ 2013 x86 Redistributable – 12.0
- Microsoft VSS Writer for SQL Server 2014
- SQL Server Browser for SQL Server 2014

**To uninstall FortiClient EMS:**

1. Select *Start* > *Control Panel* > *Programs* > *Uninstall a program*.
2. Select *FortiClient Enterprise Management Server*, and click *Uninstall*.
3. Follow the uninstallation wizard prompts.

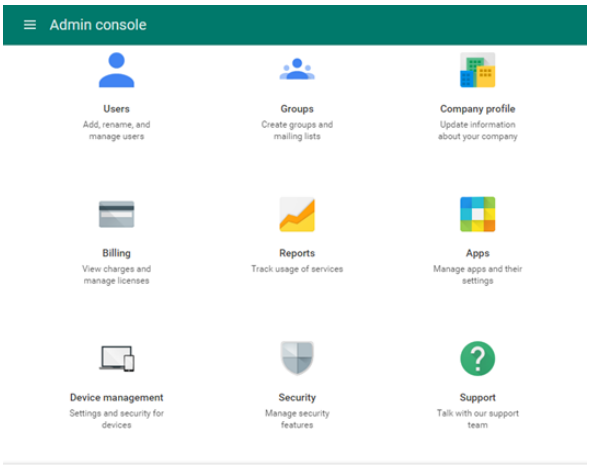
# Google Admin Console Setup

This section describes how to add and configure the FortiClient Web Filter extension on Chromebooks that are enrolled in the Google domain.

## Logging in to the Google Admin console

**To log in to the Google Admin console:**

1. Log in to the Google Admin console (https://admin.google.com) by using your Google Domain admin account. The Admin console is displayed.



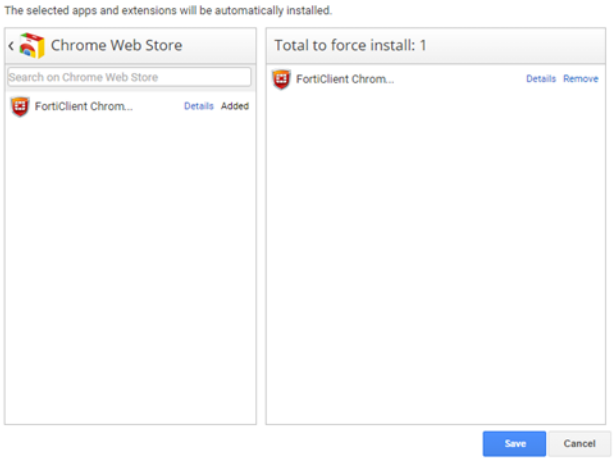

## Adding the FortiClient Web Filter extension

FortiClient EMS for Chromebooks software is not available for public use. You can only enable the feature by using the following extension ID: igbg-pehnbmhgdgjbhkkpedommgmfbeao

**To add the FortiClient Web Filter extension:**

1. In Google Admin console, go to *Device management* > *Chrome Management* > *User Settings* > *Apps and Extensions* > *Force-installed Apps and Extensions* > *Manage force-installed apps*.
2. Select *Chrome Web Store*, and search for the following extension ID: igbgpehnbmhgdgjbhkkpedommgmfbeao.
3. Add the extension ID and save.

The extension name is displayed as *FortiClient Chromebook Web Filter Extension*.




## Configuring the FortiClient Web Filter extension

You must configure the FortiClient Chromebook Web Filter extension to enable Google Admin console to communicate with FortiClient EMS for Chromebooks.

FortiClient EMS for Chromebooks hosts the services that assign web-filter policies to groups in the Google domain. FortiClient EMS for Chromebooks also handles the logs and web-access statistics sent from the extensions.

FortiClient EMS for Chromebooks is the profile server.

**To configure the FortiClient Web Filter extension:**

1. In FortiClient EMS for Chromebooks, locate the server name and port by going to *View* > *Settings*.
2. Create a text file that contains the following text:

```
{
   "ProfileServerUrl": { "Value": "https://< ProfileServer >:< port for Profile Server >"}
}
```

   For example:

```
{
   "ProfileServerUrl": { "Value": "https://ems.mydomain.com:8443”}
}
```

3. In Google Admin console, go to *Device management* > *Chrome Management* > *App Management* > *FortiClient Chrome Web Filter Extension* > *User settings*.
4. Click a domain or organization unit (OU).
5. In the right pane, under *Configure*, upload a new configuration file.

   You can also view the current settings.
6. Click *Save*.

   Go to *Device Management* > *Chrome* > *App Management*, to view your configured Chrome apps.

# Adding root certificates

This section includes:



## Communication with FortiClient Chromebook Web Filter extension

The FortiClient Chromebook Web Filter extension communicates with FortiClient EMS for Chromebooks by using HTTPS connections. The HTTPS connections require an SSL certificate. You must obtain an SSL certificate and add the certificate to FortiClient EMS for Chromebooks to allow the extension to trust FortiClient EMS for Chromebooks. See SSL certificates on page 17.

If you use a public SSL certificate, you only need to add the public SSL certificate to FortiClient EMS for Chromebooks. See Adding SSL certificates on page 40.

However, if you prefer to use a certificate that is not from a common CA, you must add the SSL certificate to FortiClient EMS for Chromebooks, and you must also push the root CA of your certificate to the Google Chromebooks. Otherwise, the HTTPS connection between the FortiClient Chromebook Web Filter extension and FortiClient EMS for Chromebooks will not work. Please refer to Uploading a root certificate to Google Admin Console on page 26 on how to upload a root certificate.

## Communication with FortiAnalyzer for logging

This section applies only if you are sending logs to FortiAnalyzer. If you are not sending logs, you can skip this FortiAnalyzer section.

Sending logs to FortiAnalyzer requires that you enable ADOMs in FortiAnalyzer and add FortiClient EMS for Chromebooks to FortiAnalyzer. FortiClient EMS for Chromebooks is added as a device to the FortiClient ADOM in FortiAnalyzer. For information on enabling ADOMs and adding a device to FortiAnalyzer, see the *FortiAnalyzer Administration Guide*.

The FortiClient Chromebook Web Filter extension communicates with FortiAnalyzer by using HTTPS connections. The HTTPS connections require an SSL certificate. You must obtain an SSL certificate and add the certificate to FortiAnalyzer to allow the extension to trust FortiAnalyzer.

If you use a public SSL certificate, you only need to add the public SSL certificate to FortiAnalyzer.

However, if you prefer to use a certificate that is not from a common CA, you must add the SSL certificate to FortiAnalyzer, and you must also push the root CA of your certificate to the Google Chromebooks. Otherwise, the HTTPS connection between the FortiClient Chromebook Web Filter extension and FortiAnalyzer will not work. Please refer to Uploading a root certificate to Google Admin Console on page 26 on how to upload a root certificate.

**To add SSL certificates to FortiAnalyzer:**

The FortiAnalyzer IP address should be specified in the SSL certificate. If you're using a public SSL certificate, the FortiAnalyzer IP address can be assigned to either *Common Name* or *Alternative Name*. If you're using a self-signed (non-public) SSL certificate, the *Subject Alternative Name* of your certificate must include `IP:<FortiAnalyzer IP>`.

In FortiAnalyzer,

1. Go to *System Settings* > *Certificates* > *Local Certificates*.
2. Click *Import*. The *Import Local Certificate* dialog box appears.
3. In the *Type* list, select *Certificate*. Or,
   In the *Type* list, select *PKCS #12 Certificate* to upload the certificate in PK12 format.
4. Beside *Certificate File*, click *Browse* to select the certificate.
5. Enter the password and certificate name.
6. Click *OK*.

**To select certificates for HTTPS connections:**

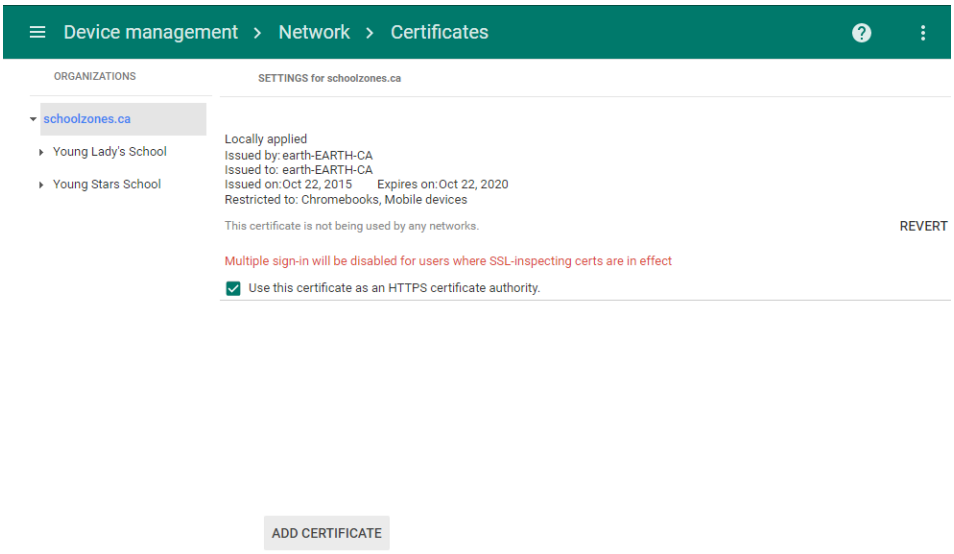
In FortiAnalyzer,

1. Go to System *Settings* > *Admin* > *Admin Settings*.
2. In the *HTTPS & Web Service Certificate* box, select the certificate you want to use for HTTPS connections, and click *Apply*.

## Uploading a root certificate to Google Admin Console

1. In Google Admin console, go to *Device Management* > *Network* > *Certificates (root certificate) (crt certificate)*.
2. Add the root certificate.
3. Select the *Use this certificate as an HTTPS certificate authority* checkbox.

Do not forget to select the *Use this certificate as an HTTPS certificate authority* checkbox.




## Disabling access to Chrome developer tools

It is recommended to disable access to Chrome developer tools. This blocks students from disabling the FortiClient Web Filter extension.

**To disable access to Chrome developer tools:**

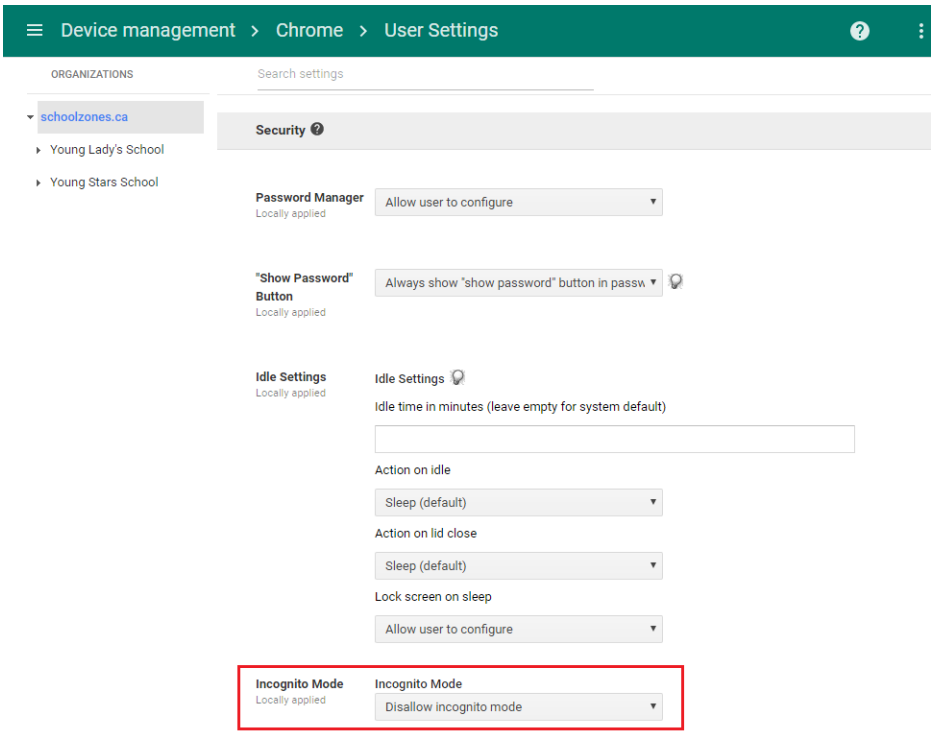
1. In the Google Admin console, go to *Device management* > *Chrome Management* > *User Settings*.
2. For the *Developer Tools* option, select *Never allow user of built-in developer tools*.

## Disallowing incognito mode

When users browse in incognito mode, extensions will be bypassed. Incognito mode should be disallowed for managed Google domains.

**To disallow incognito mode:**

1. In the Google Admin console, go to *Device management* > *Chrome management* > *User settings*.
2. On the left, select the organization.
3. In the *Security* section, set *Incognito Mode* to *Disallow incognito mode*.



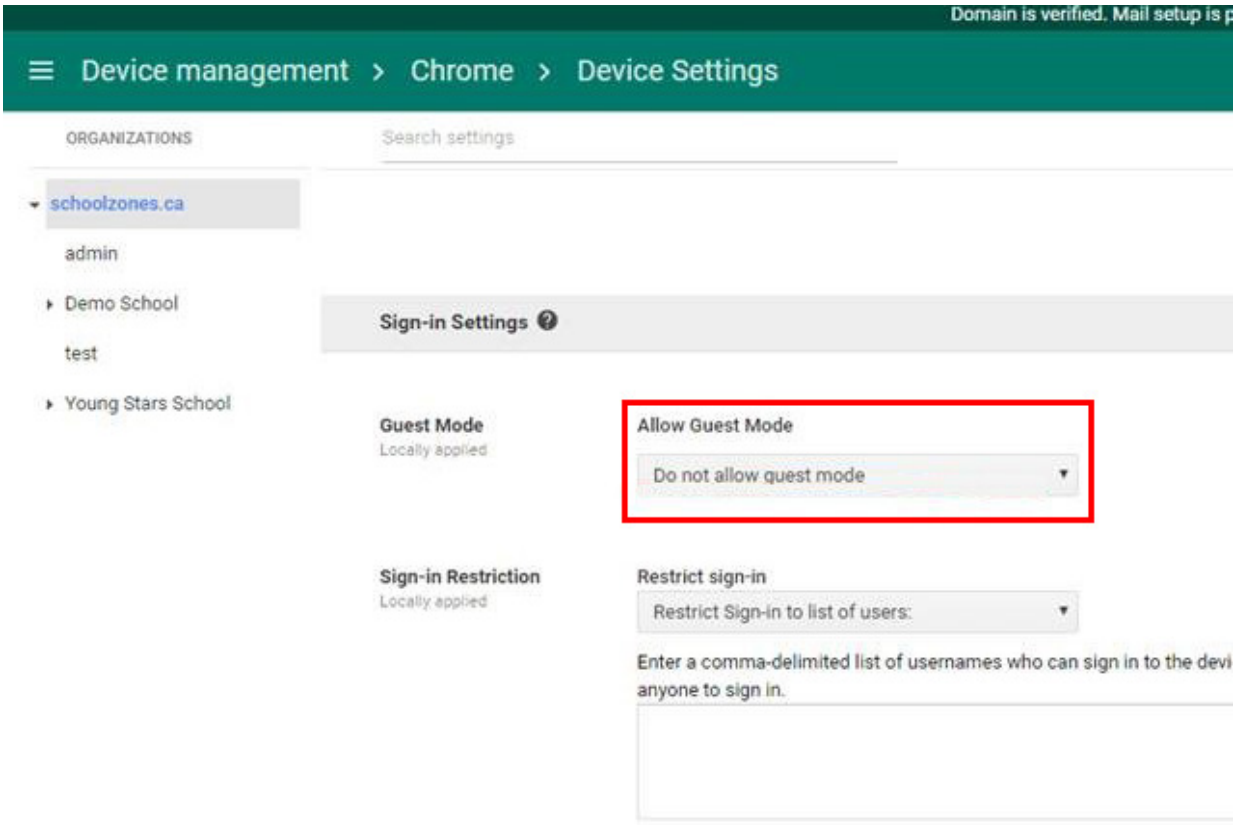

4. Click *Save*.

## Disallowing guest mode

Guest mode should be disallowed for managed Google domains.

**To disallow guest mode:**

1. In the Google Admin console, go to *Device management* > *Chrome management* > *Device settings* > *Sign-in settings*.
2. From the left panel, select the organization.
3. Under *Guest Mode* > *Allow Guest Mode* > select *Do not allow guest mode* from the dropdown.



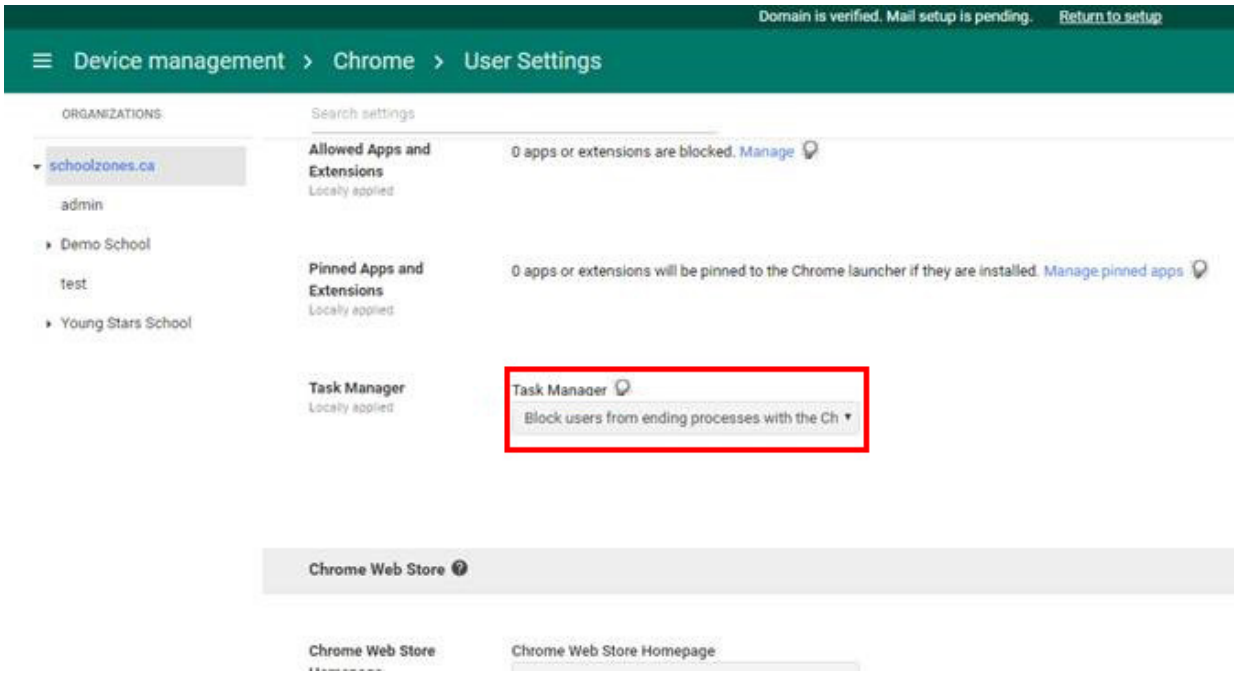

4. Click *Save*.

## Blocking Task Manager

Task Manager should be blocked for managed Google domains.

**To block Task Manager:**

1. In Google Admin console, go to *Device Management* > *Chrome Management* > *User settings* > *Apps and Extensions*.
2. From the left panel, select the organization.
3. Under *Task Manager* select *Block users from ending processes with the Chrome Task Manager* from the dropdown.



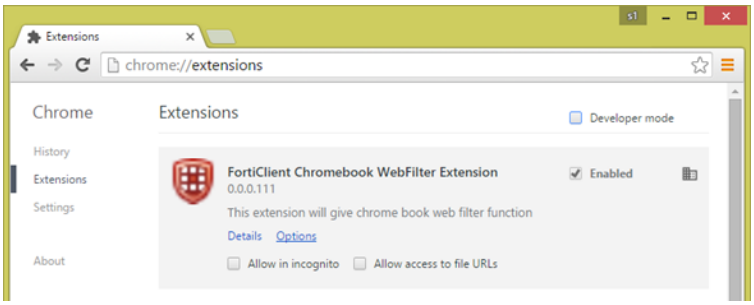

4. Click *Save*.

## Verifying the FortiClient Web Filtering extension

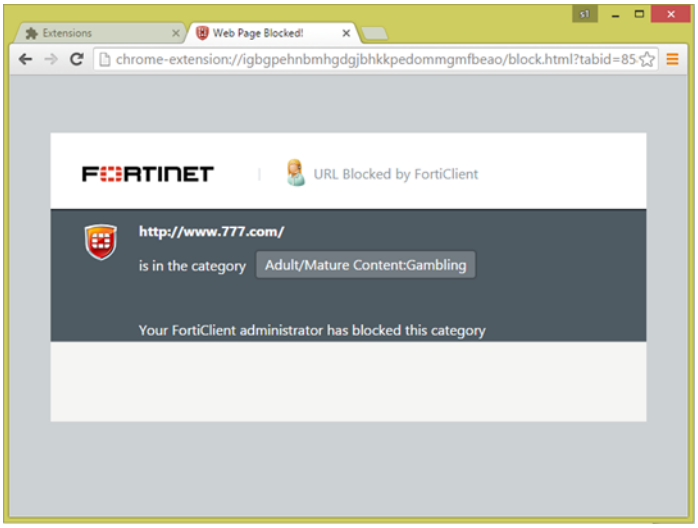
After you add the Google domain to FortiClient EMS for Chromebooks, the Google Admin console automatically pushes the FortiClient Web Filtering extension to the Chromebooks when users log into the Google domain. You can verify that the feature is available in Chromebooks.

**To verify that the extension is installed:**

1. Open the Google Chrome browser.
2. Type the following in the address bar: *chrome://extensions*



3. Visit any gambling site, such as http://www.777.com, and confirm that the site is blocked.



# Service Account Credentials

FortiClient EMS for Chromebooks requires service account credentials generated by the Google Developer console. You can use the default service account credentials provided with FortiClient EMS for Chromebooks, or you can generate and use unique service account credentials, which is more secure.


- Configuring default service account credentials on page 32
- Configuring unique service account credentials on page 32


The service account credentials must be the same in FortiClient EMS for Chromebooks and the Google Admin console.

## Configuring default service account credentials

FortiClient EMS for Chromebooks includes the following default service account credentials generated by the Google Developer console:

| Option | Default Setting | Where Used |
|---|---|---|
| Client ID | 102515977741391213738 | Google Admin console |
| Email address | account-1@forticli-entwebfilter.iam.gserviceaccount.com | FortiClient EMS for Chromebooks |
| Service Account Certificate | A certificate in `.pem` format for the Service Account Credentials | FortiClient EMS for Chromebooks |

### Adding the default service account client ID in Google Admin console

If you decide to use the default service account credentials, you do not need to change the service account certificate and email in EMS, but you must configure the client ID with the default value in the Google Admin console. See Adding service account credentials to the Google Admin console on page 36.

The service account credentials are a set. If you change one of the credentials, you must also change the other two credentials.

## Configuring unique service account credentials

When using unique service account credentials for improved security, you must complete the following steps to add the unique service account credentials to the Google Admin console and FortiClient EMS for Chromebooks:

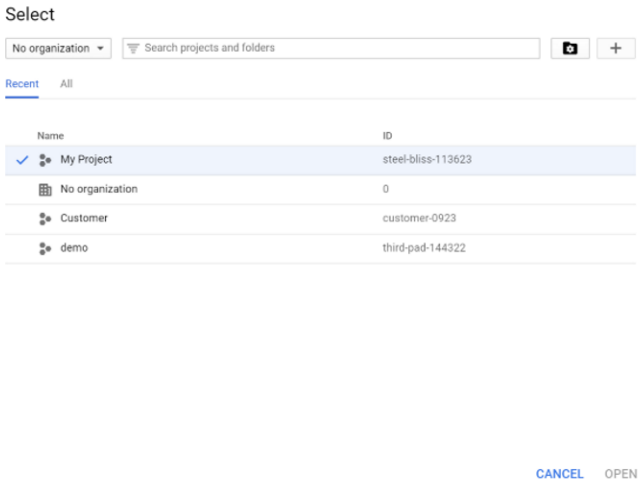
1. Create unique service account credentials by using the Google Developer console. See Creating unique service account credentials on page 33.
2. Add the unique service account credentials to the Google Admin console. See Adding service account credentials to the Google Admin console on page 36.
3. Add the unique service account credentials to FortiClient EMS for Chromebooks. See Adding service account credentials to FortiClient EMS on page 37.

## Creating unique service account credentials

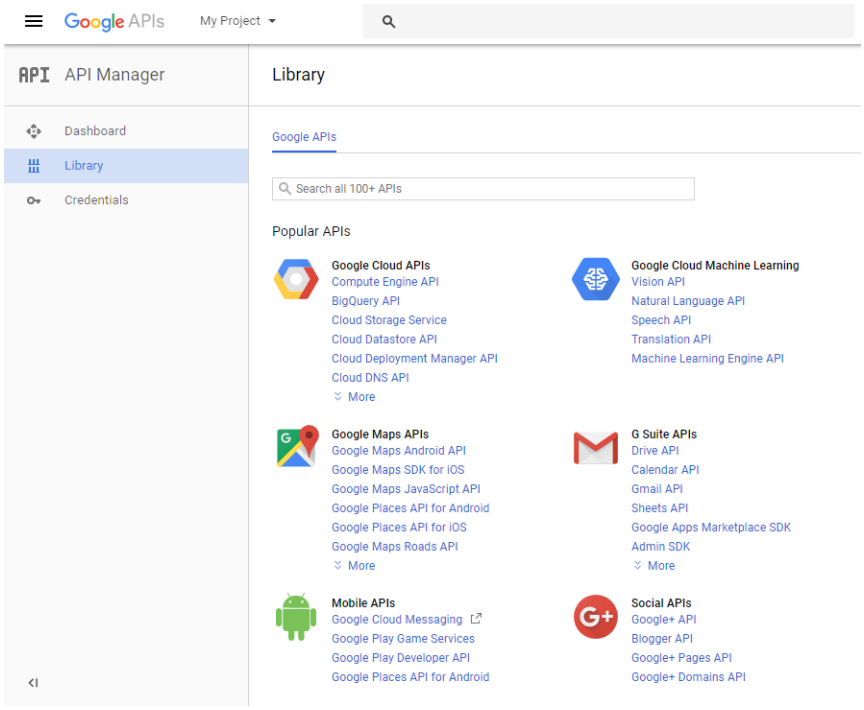
Creating a unique set of service account credentials provides more security. To create a unique service account, follow the procedure below.

**To create a unique service account:**

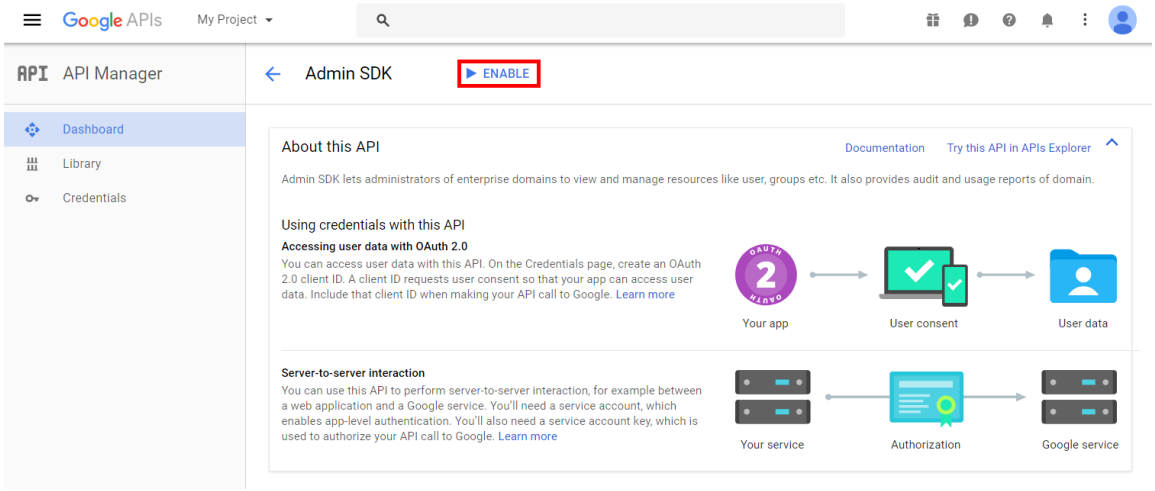
1. Go to https://console.developers.google.com.
2. Log in with your Google for Work account credentials.
3. Create a new project.
   a. Click the toolbar list. The browser displays the following dialog.




   b. Select your organization, if you see an organization dropdown list.
   c. Click the + button.
   d. In the *Project name* field, enter your project name, then click *Create*.
4. Enable the Admin SDK.
   a. Select your project from the toolbar list, then go to the *Library* tab.
   b. Under *G Suite APIs*, click *Admin SDK*.




**c.** Click *ENABLE*.



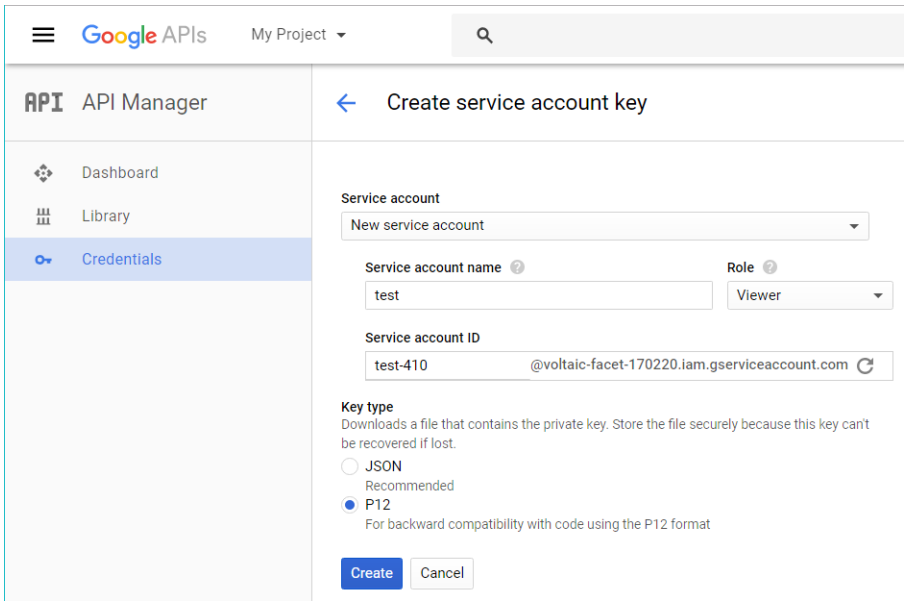

**5.** Create a service account.

**a.** Go to the *Credentials* tab and select *Create Credentials* > *Service account key*.

**b.** From the *Service account* list, select *New Service Account*. Enter a service account name.

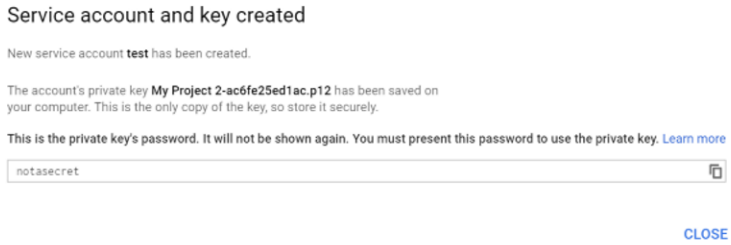
**c.** From the *Role* list, select *Project* > *Viewer*.

**d.** Select *P12* as the *Key type* and click *Create*.

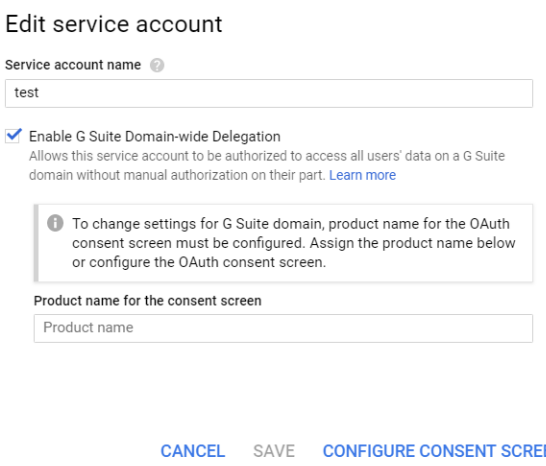



After you create the service account, a private key with the `P12` extension will be saved on your computer.

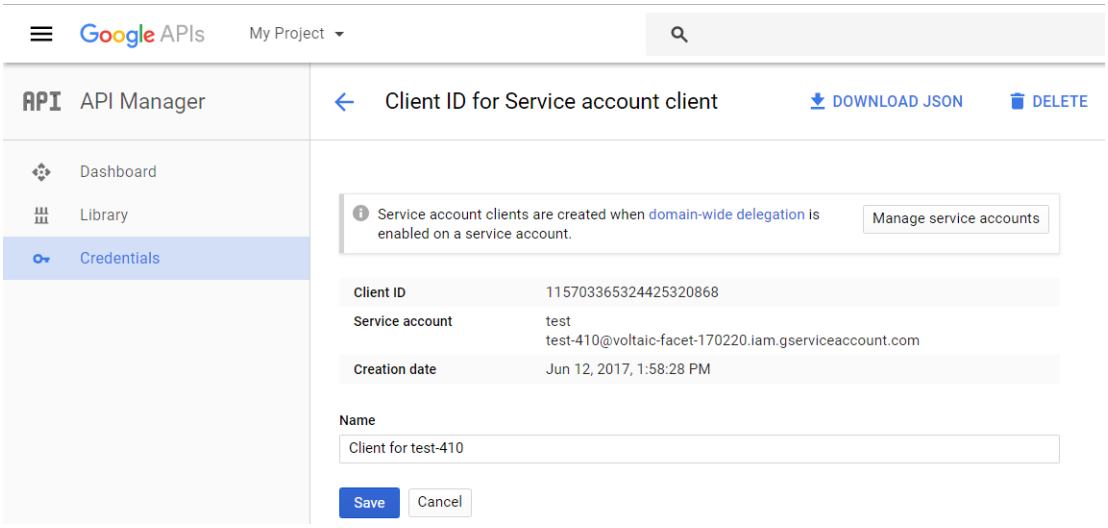
> ⚠ The private key with the `P12` extension is the only copy you will receive. Keep it in a safe place. You should also remember the password prompted on the screen. At this time, that password should be **`notasecret`**.




6. Go to the *Credentials* page > *Manage service accounts*.
7. *Edit* the service account you just created and enable the *Enable Google Apps Domain-Wide Delegation* checkbox. Enter a *Product name for the consent screen* if this field appears.




8. Click *Save*.
9. Click *View Client ID*, and you will see your service account information. Record the client ID, service account, and the associated private key (downloaded in step 5d).




To use the private key in FortiClient EMS, it needs to be converted to `.pem` format. You can use the following `openssl` command to convert it. Remember to use the not-asecret password.

```
C:\OpenSSL-Win64\bin>openssl pkcs12 -in demo-
    976b9d6e9328.p12 -out serviceAccount-demo.pem -nodes -
    nocerts
Enter Import Password:
```

## Adding service account credentials to the Google Admin console

You must add the client ID from the default or unique service account credentials. The default or unique service account credentials, including the client ID, must be the same in FortiClient EMS for Chromebooks and the Google Admin console.

These settings allow Google to trust FortiClient EMS for Chromebooks, which enables FortiClient EMS for Chromebooks to retrieve information from the Google domain.

**To add the client ID:**

1. In the Google Admin console, go to *Security* > *Advanced settings* > *(you might need to click "show more" to see this)* > *Manage API client access*.
2. Set the following options:
   a. For the *Client Name* option, add the client ID from the server account credentials.
   b. For the *API Scopes* option, add the following string:
   https://www.googleapis.com/auth/admin.directory.orgunit.readonly,https://www.googleapis.com/auth/admin.directory.user.readonly

The API Scopes are case-sensitive and must be lowercase.

You might need to copy the string into a text editor and remove spaces created by words wrapping to the second line in the PDF.

3. Click *Authorize*.

## Adding service account credentials to FortiClient EMS

The section describes how to add the service account ID and the service account certificate from the service account credentials to FortiClient EMS for Chromebooks.

**To add service account credentials:**

1. In FortiClient EMS for Chromebooks, go to *View* > *Settings*.
2. Click *EMS for Chromebook*, and set the following options:

The default service account credentials are displayed. Overwrite the default settings with the unique set of service account credentials that you received from Fortinet.

| | |
|---|---|
| Service Account Certificate | Click *Browse*, and select the certificate provided with the service account credentials. |
| Service Account ID | Type the email address provided with the service account credentials. |

3. Click *Save*.
4. Update the client ID in the Google Admin console.

The service account credentials are a set. If you change one of the credentials, you must also change the other two credentials.

# GUI

## Navigating the FortiClient EMS for Chromebooks interface

FortiClient EMS for Chromebooks offers a centralized view of managing Chromebooks and allows you to define and make endpoint security profile changes.

The application provides views or panes in which you can manage endpoints and profiles, such as domain profile, and content pane views. You can switch between these views according to your needs. The user interface is a graphical summary of important security information about the endpoint clients in your organization.

### Banner

| Option | Description |
|---|---|
| License Type | Displays current license information. |
| Envelope icon | Clicking the Envelope icon displays all Alerts. |
| View | View and configure the following:<br>• Upgrade License<br>• User Management<br>• Database Management<br>• View Logs<br>• Settings |
| Help | View the following:<br>• Technical Documentation<br>• How-To Videos<br>• Forums<br>• Getting Started<br>• Create Support Package<br>• About |
| Admin | Logout of FortiClient EMS. |

### Left pane

The left navigation pane is used to display content in the right content pane.

| Option | Description |
|---|---|
| Dashboard | Display a dashboard of information about all managed FortiClient end-points. |
| Google Domains | Add and manage Google domains. |
| Endpoint Profiles | Create and assign profiles as well as manage profile updates. |

## Right pane

The right content pane displays the user interface controls that correspond to the selection you make in the left navigation pane. The status and menu icons on the top-right display controls that you can use to configure additional settings for user management and each individual endpoint.

**To view the dashboard:**

1. Click the *Dashboard* on the left pane. A summary of the status of the endpoints is displayed.
2. Click any of the pie charts to view more details about the summarized endpoints.
3. Click any of the displayed endpoints to view more details about the endpoint.

### License information

| Option | Description |
|---|---|
| License Information | Displays the following information:<br>• Status of your License<br>• Expiration Date<br>• Number of Licenses |

### Charts

In the right pane, there are a number of pie charts. Each pie chart provides a summary of endpoint information. The sections in each of the charts are links. You can click any section of the pie charts or any row in the table to display more details.

| Option | Description |
|---|---|
| Client Stats | Statistics of Clients in use. |
| Top 10 Web Filter Violations by Category | The chart displays the top 10 Web Filter Violations by Category. |
| Top 10 Web Filter Violation by User | The chart displays the top 10 Web Filter Violations by User. |

# Settings

This section describes FortiClient EMS for Chromebooks server settings and log settings. It also describes how to import CA certificates as well as back up and restore the database.

## FortiClient EMS for Chromebooks settings

### Server settings

FortiClient EMS for Chromebooks installs with a default IP address and port configured. You can change the IP address and port, and configure other server settings for FortiClient EMS for Chromebooks.

**To configure server settings:**

1. Go to *View* > *Settings*.
2. Select *Server Settings*, and configure the options. For a description of the options, see the Server Settings on page 42.
3. Select *Save*.

### Log settings

You can specify what level of log messages to capture in the logs for FortiClient EMS for Chromebooks. You can also specify when to automatically delete logs and alerts.

**To configure log settings:**

1. Go to *View* > *Settings*.
2. Under *Log Settings*, configure the options. For a description of the options, see Log Settings on page 42.
3. Select *Save*.

### EMS for Chromebook

To Add Unique Service Account Client ID in Google Admin console, see Adding service account credentials to the Google Admin console on page 36.

Once you have added the Unique Service Account Credentials to Google Admin Console, you need to update the Unique Service Account Credentials to EMS. See Adding service account credentials to FortiClient EMS on page 37

#### Adding SSL certificates

You must add an SSL certificate to FortiClient EMS for Chromebooks to allow HTTPS connections with Google Admin console. See also SSL certificates on page 17.

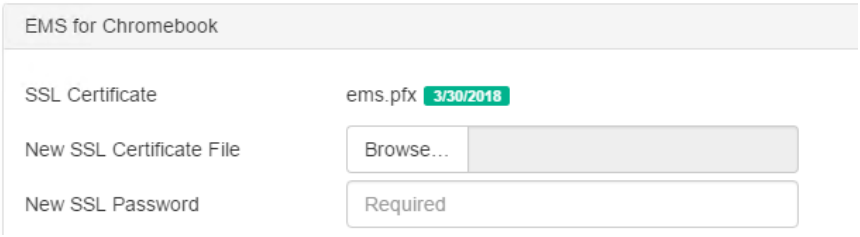
If you are using a public SSL certificate, add the certificate to FortiClient EMS for Chromebooks. You do not need to add the certificate to Google Admin console.

If you are not using a public SSL certificate, you must add the SSL certificate to FortiClient EMS for Chromebooks, and you must add the root certificate to Google Admin console. See Adding root certificates on page 25.

**To add or replace SSL certificates:**

1. In FortiClient EMS, go to *View >Settings*.
2. Click the *EMS for Chromebook*.
3. Beside *New SSL Certificate File*, click *Browse*, and locate the certificate file (server.pfx) and its password.
4. Click *Save*.

If the SSL certificate is expiring in less than three months, the expiry date label will be yellow; if it has expired, the label will be red. Otherwise, it is green.




**To configure the other settings:**

1. Go to *View* > *Settings*.
2. Under *EMS for Chromebook*, configure the options. For descriptions of the options, see EMS for Chromebook on page 42
3. Click *Save*.

## Email alert settings

You can add an option to setup an SMTP server to enable an Alert for EMS Events. When an alert is triggered, an email notification will be sent.

**To configure email alerts and an SMTP server**

1. Go to *Settings* > *Alerts* > *Email Alerts*
2. Enable *Send e-mail alerts for the following EMS*.
3. Select the *Alert* types you would like to receive an email notification for.
4. Click *Save*.
5. If you have not already set up an SMTP Server, the GUI will automatically prompt you to configure the *SMTP Server Settings* information. See the Configuration references on page 41.
6. Click *Save*.

# Configuration references

This section contains descriptions of the fields used to configure FortiClient EMS for Chromebooks.

## Server Settings

Following is a description of the fields on the *View* > *Settings* > *Server Settings* tab.

| Option | Description |
|---|---|
| Remote administration/HTTPS Access | Specify settings for remote administration access to FortiClient EMS for Chromebooks.<br><br>Turn remote HTTPS access to FortiClient EMS for Chromebooks console on and off. When enabled, administrators can use a browser and HTTPS to log into the FortiClient EMS for Chromebooks console. When disabled, administrators can only log into FortiClient EMS for Chromebooks console on the server. |
| SSL Certificate | Displays the SSL Certificate currently imported. If you have not imported a SSL Certificate, a *No SSL certificate imported* message is displayed. |
| New SSL Certificate | Upload a new SSL Certificate. |
| New SSL Private Key | Upload a new SSL Private Key. |
| User Inactivity Timeout | Specify the user inactivity timeout (in hours). |

## Log Settings

Following is a description of the fields on the *View* > *Settings* > *Log Settings* tab.

| Option | Description |
|---|---|
| Log level | Select the level of messages to include in FortiClient EMS for Chromebooks logs. For example, if you select *Info*, all log messages from *Info* to *Emergency* are added to the FortiClient EMS for Chromebooks logs. |
| Auto Remove Logs | Type the number of days that you want to store logs. For example, if you type 30, logs will be stored for 30 days. Any logs older than 30 days are automatically deleted. |
| Remove All Logs | Click to immediately delete all FortiClient EMS for Chromebooks logs. |
| Auto Remove Web Filter Violations | Type the number of days that you want to keep violations. For example, if you type 30, violations will be kept for 30 days. Any violations older than 30 days are automatically deleted. |

## EMS for Chromebook

Following is a description of the fields on the *View* > *Settings* > *EMS for Chromebook* tab.

| Option | Description |
|---|---|
| SSL Certificate | Displays the SSL Certificate currently imported. . If you have already uploaded a SSL certificate a *Replace* button is displayed. |
| New SSL Certificate File | Browse and upload a new SSL Certificate File. |
| New SSL Password | Configure a new SSL Password. |
| Listen on Port | Displays the default port for the FortiClient EMS for Chromebooks server. You can change the port by typing a new port number. FortiClient will connect to EMS by using the specified port number. |
| Profile Update Interval | Specify the profile update interval (in seconds). |
| Service Account ID | Displays the Service Account ID currently in use. |
| New Service Account ID | Enter a new Service Account ID. |
| New Service Account Private Key | Enter a new Service Account Private Key. |
| Reset | In the event your service account is broken, you can revert back to the default service account by clicking the *Reset* button. This restores the default service account. You will need to *Save* the settings for the change to take effect. |

## Email Alerts

Following is a description of the field for *View > Settings > Alerts > Email Alerts > Send e-mails alerts for the following EMS events*.

| Option | Description |
|---|---|
| Notify when new EMS versions are available for deployment | New EMS versions are available. |
| Remind me everyday for 2 weeks | Enable to remind you when new EMS versions are available everyday for 2 weeks. |
| Notify when EMS license is expiring or expired. | Expiring or expired EMS license. |

## SMTP Server Settings

Following is a description of the fields on the *View > Settingrs > Alerts > Enable send email alerts for the following EMS events > SMTP Server Settings*. You will need to enable *Enable send an email for the following*

*EMS events* to show the SMTP Server Settings.

| Option | Description |
|---|---|
| SMTP Server | Enter SMTP Server. |
| Port | Enter Port number. |
| Security | Select either *None*, *STARTTLS*, or *SMTPS* for the security type, or you can select the *Auto-Detect* button to automatically select the security type. |
| Username | Enter Username. |
| Password | Enter Password. |
| From Address | Enter From Address. |
| Reply-To | Enter Reply Address. |
| Subject | Subject of the sent e-mail alert. |
| Recipient(s) | Enter email address(es) to send Alerts to. Click the + button to add more email addresses. |
| Test Email Settings | Click the button to test the Email Settings. |

# User Management

This section describes the default user accounts and permissions for FortiClient EMS for Chromebooks. It also describes how to change the administrator password and how to configure Windows users.

## Default user accounts and permissions

The administrator has complete access to all FortiClient EMS permissions, including modification, user permissions, approval, discovery, and deployment.

## Configuring User Management

### Changing the administrator password

By default, the password is blank for the administrator account. You should add a password to increase security.

**To change the administrator password:**

1. Go to *View* > *User Management*.
2. On the *Administration* tab, select the *Admin* account.
3. Click *Change Password* from the toolbar.
4. Change your password, and click *Save*.

### Configuring Windows user accounts

You can configure Windows users to have no access to FortiClient EMS for Chromebooks, or you can configure Windows users to have administrator access to FortiClient EMS for Chromebooks.

The list of Windows users is derived from the server on which FortiClient EMS for Chromebooks is installed. If you want to add more Windows users, you must add them to the server.

**To configure Windows users:**

1. Go to *View* > *User Management*.
2. On the *Administration* tab, click the *+Add* button from the toolbar.
3. From the *Add User* dropdown menu, select the Windows user.
4. Perform one of the following actions:
    a. Select the specific domain access for the user. For a description of the permissions, see Default user accounts and permissions on page 45.
    b. Configure the permissions.
5. Click *Save*.

# User Management reference

This section contains descriptions of the fields used to configure user management.

## Administration

Following is a description of the fields on the *View* > *User Management* > *Administration* tab.

| Option | Description |
|---|---|
| +Add | Add a new user. |
| Name | Name of the user. |
| Access | Type of user access. |
| Type | Type of user. |

## Windows Users

Following is a description of the fields on the *View* > *User Management* > *Add* > *User*.

| Option | Description |
|---|---|
| Add User | Select the User for whom you want to configure permissions for FortiClient EMS for Chromebooks. |
| Super Administrator Permissions | Enable the Super Administrator feature to give the new Windows Users Super Administrator permissions. |
| Comments | Enter optional comments/information for the Windows User. |
| Domain Access | Select or add a Domain Access for the Windows and configure their permissions.<br><br>If you choose one or more domains in the domain access field, you will need to select specific permissions. |
| Permissions | Use the settings to configure permissions to FortiClient EMS for Chromebooks for the selected Windows User. |
| General | |
| Create / Delete Filters | Select to allow the Windows user to create and delete filters. Clear to disable this permission. |

| Option | | Description |
|---|---|---|
| Policies | | |
| | Assign / Unassign Policy / | Select to allow the Windows user to assign to endpoints and unassign profiles from domains as well as manage custom groups. Clear to disable this permission. |
| | Create / Delete / Edit / Rename Policy | Select to allow the Windows user to create, delete, edit, and rename profiles. Clear to disable this permission. |

## Global Settings

Following is a description of the fields on the *View* > *User Management* > *Global Settings* tab.

| Option | Description |
|---|---|
| Inactivity Timeout | Specify how long to keep inactive users logged into FortiClient EMS for Chromebooks. When the time expires, the user is automatically logged out of FortiClient EMS for Chromebooks. Type 0 to keep inactive users logged into FortiClient EMS for Chromebooks indefinitely. |

# Domains

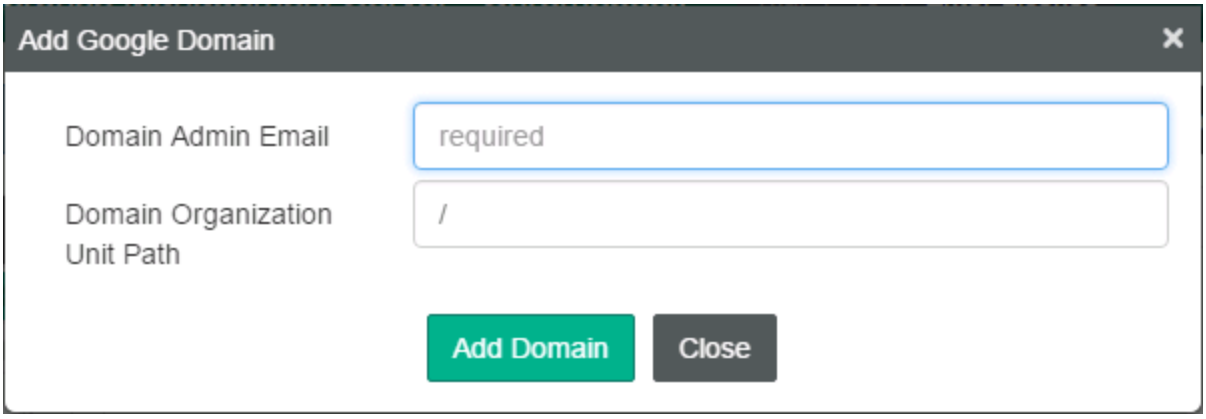
FortiClient Enterprise Management System (FortiClientEMS) needs to determine which devices it has to manage. Device information comes from the Google Admin Console.

## Adding Google domains

**To add Google domains:**

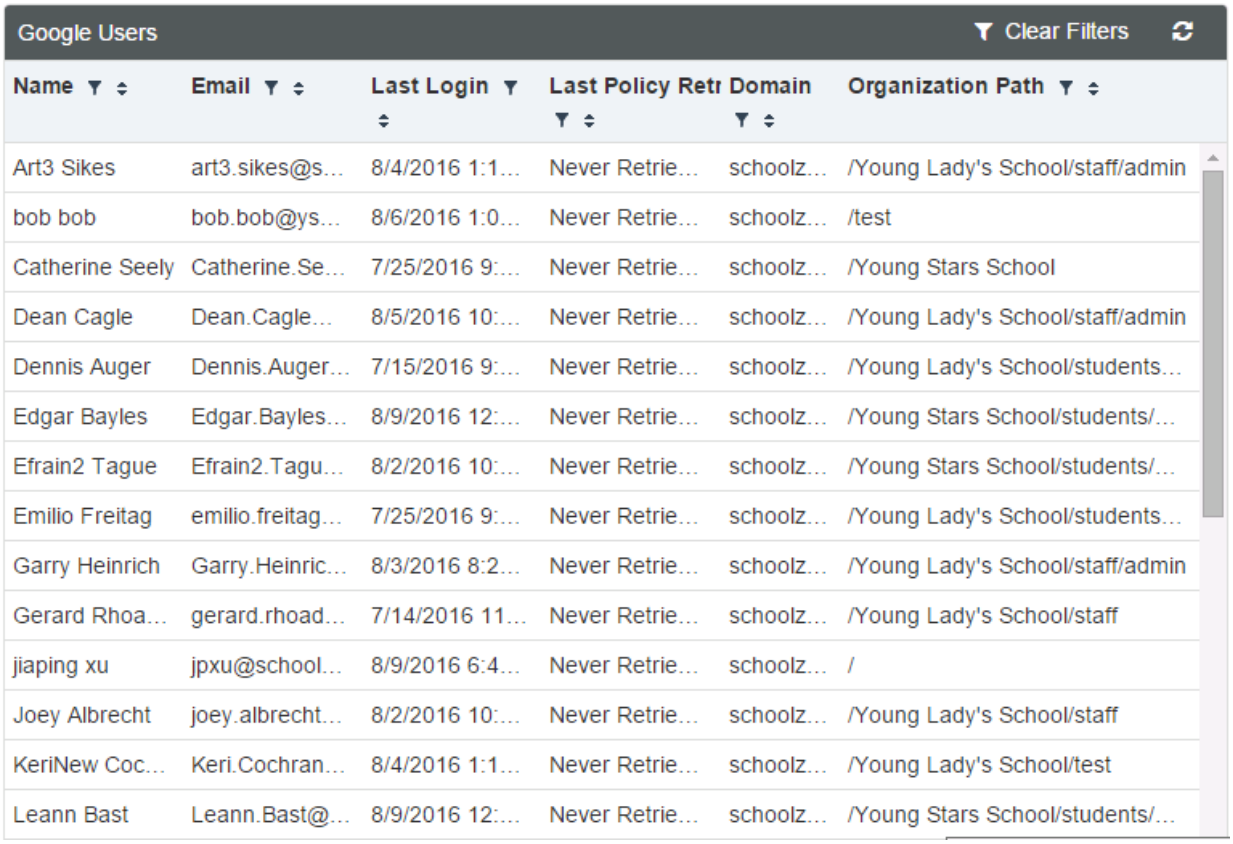
1. In FortiClient EMS for Chromebooks, in the *Google Domains* area, click the *Add a new Google domain* icon.
2. In the *Domain Admin Email* box, type your Google domain admin email, and type the *Domain Organization Unit Path*, and click *Add Domain*.

/ stands for the root of the domain.




The Google domain information and users are imported into FortiClient EMS for Chromebooks. Following is

an example of an imported Google domain:




**To view domains:**

1. Go to *Google Domain* > *select a Domain tree* to view all Chromebooks in the domain.
2. Select an endpoint to view its details.

## Managing domains

You can manage domains from the *Google Domain* pane. Some options are available as buttons, and some options are available in the right-click menu. Right-click a domain to display the menu.

| Option | Description |
|---|---|
| Refresh | Refresh the list of domains. |
| Clear Filter | Click to clear the filters. |
| Add a New Domain | Click to add a new Google Domain FortiClient EMS for Chromebooks. |
| Assign profile | Select and apply a profile to the selected domain. |
| Unassign profile | Select to unassign a profile from a selected domain. |

# Domain information

## Viewing domain information

You can view Domain information within FortiClient EMS. Use the right content pane to review the following Domain information:

- Sub Organization Structure
- Individual User Information

**To view domain information:**

Go to *Domain* > *select a Domain*. A list of information about the Domain is displayed.

The following options are available:

| Option | Description |
|---|---|
| Clear Current Filter (filter icon) | Click the Clear Current Filter icon to clear the currently used filter. |
| Refresh | Click the Refresh icon to refresh the page. |

The following information is displayed:

| Google Users | Information |
|---|---|
| Name | Name of the Chromebook user. |
| Email | Email address of the Chromebook user. |
| Last Login | Last time the Chromebook user logged in. It is date and time stamped. |
| Last Policy Retrieval | Last policy the Chromebook user retrieved. |
| Domain | Name of the domain the Chromebook is assigned to. |
| Organization Path | The organization path the Chromebook is assigned to. |

| Client Statistics | Information |
|---|---|
| Blocked Sites Distribution | The distribution of blocked sites visited by the Chromebook user. |
| Top 10 Site Categories Distribution | The top 10 site categories visited by the Chromebook user. |

| Blocked Sites (Past <number> Days) | Information |
|---|---|
| Time | The time the blocked site was visited. |
| Threat | The type of threat detected. |
| Client Version | The Chromebook User's current version. |
| OS | The type of OS used by the Chromebook user. |
| URL | The URL of the blocked site. |
| Port | The port number currently listening. |
| User Initiated | User initiated visitation to the blocked site. |

# Profiles

## Configuring profiles

The profile currently supports web filtering by categories, black and white list, and safe search. You can create different profiles and assign the profiles to different groups in the Google domain.

### Adding new profiles

When you install FortiClient EMS, a default profile is created. This profile is applied to any domains that you create.

It is recommended to add Yandex search engine to the black list in the profile.

**To create new profiles:**

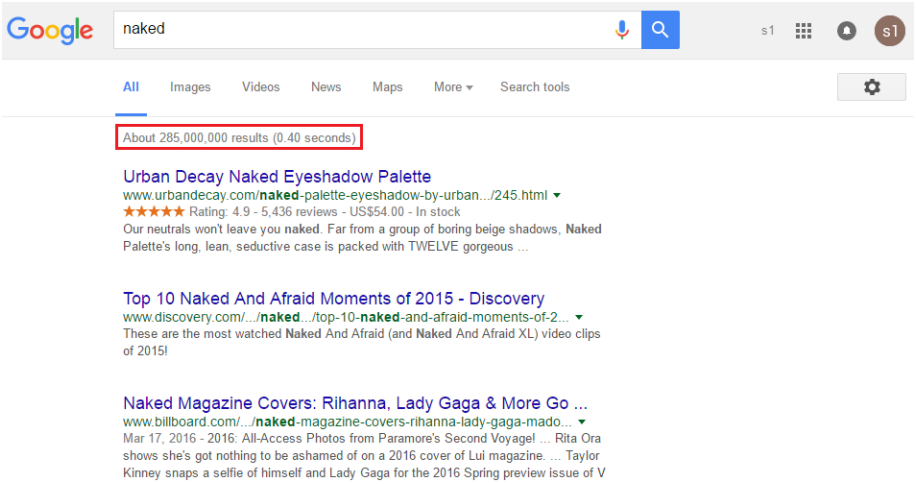
1. Go to *Endpoint Profiles* > *EMS Profiles* > *Add a new profile*.
2. In the *Profile Name* box, type a name for the profile.
3. On the *Web Filter* tab, set the web filtering options.
4. On the *System Settings* tab, set the logging options.
   For a description of the options, see Profile references on page 55.
5. Click *Save* to save the profile.

### Enabling/disabling Safe Search

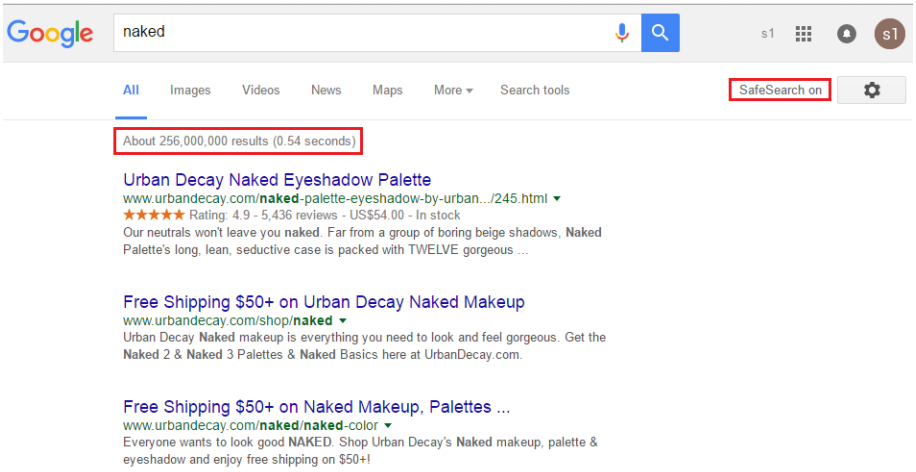
The search engine supplies a Safe Search feature that blocks inappropriate or explicit images from your search results. The Safe Search feature helps avoid most adult content. FortiClient EMS for Chromebooks supports Safe Search for most common search engines, such as Google, Yahoo, and Bing.

The profile in FortiClient EMS for Chromebooks controls the Safe Search feature.

Following are examples of search results with the Safe Search feature disabled and enabled. Notice the difference between the number of results. Here are the search results when the Safe Search feature is disabled, which has about 285,000,000 results:



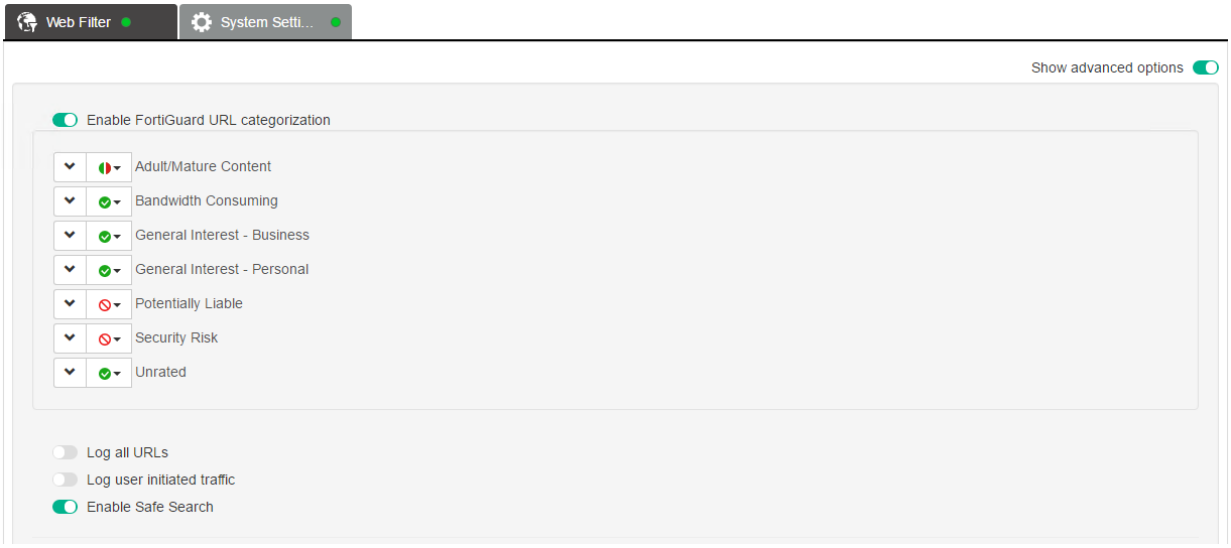

Here are the search results when the Safe Search feature is enabled, which has about 256,000,000 results.




**To enable or disable Safe Search:**

1. In FortiClient EMS for Chromebooks, in the *Endpoint Profiles* area, click the *Default* profile or another profile.
2. Enable *Show advanced options*.
3. Enable or disable the *Enable Safe Search* option.

You must enable *Show advanced options* to see the *Enable Safe Search* option.




# Pushing profile changes to Google Chromebooks

## Assigning profiles to Google Chromebooks

After creating the profile, you can assign the profile to Google Domains. When you assign the profile to domains, the profile settings are automatically pushed to the Chromebooks in the domain.

**To assign profiles:**

1. Go to *Google Domains*
2. Right-click a domain, select *Assign Profile*, and then the profile. The profile is assigned.
3. Hover the mouse over the name of the domain to view the name of the assigned profile.

## Editing profiles

When you edit a profile that is assigned to domains, the changes are automatically pushed to the Chromebooks when you save the profile.

**To update profiles:**

1. Go to *Endpoint Profiles* > *EMS Profiles*, and select a profile. The profile settings are displayed in the content pane.
2. Edit the settings. For a description of the options on the tabs, see Profile references on page 55.
3. Click *Save*. The changes are installed on the endpoints associated with the profile.

# Managing profiles

You can manage profiles from the *Endpoint Profiles* pane by clicking the icons.

| Option | Description |
|---|---|
| Refresh | Refresh the list of profiles. |
| Add a New Profile | Click to create a new profile. |
| Revert to default | Click to revert the default profile to its default settings. |
| Edit | Select a profile to display its settings in the content pane for editing. |
| Clone | Click to clone the profile. |
| Delete | Click to delete the profile. |

# Profile references

This section contains descriptions of the fields used to configure profiles.

## Endpoint Profile pane

| Configuration | Description |
|---|---|
| Profile Name | Type a name for the profile. |

### Web Filter

| Configuration | Description |
|---|---|
| Web Filter | Enable web filtering.<br>• Enable FortiGuard URL categorization: Block, Warn, Allow, or Monitor specific categories of web sites. See the FortiGuard web site for descriptions of the available categories and subcategories.<br>• Exclusion List: Enter specific URLs to block or allow. Wildcard characters and Perl Compatible Regular Expressions (PCRE) can be used. |
| Enable FortiGuard URL categorization | |

| Configuration | | Description |
|---|---|---|
| | Adult/Mature Content | Select one of the following:<br>• Block<br>• Warn<br>• Allow<br>• Monitor<br>See the FortiGuard web site for descriptions of the available categories and subcategories. |
| | Bandwidth Consuming | Select one of the following:<br>• Block<br>• Warn<br>• Allow<br>• Monitor<br>See the FortiGuard web site for descriptions of the available categories and subcategories. |
| | General Interest-Business | Select one of the following:<br>• Block<br>• Warn<br>• Allow<br>• Monitor<br>See the FortiGuard web site for descriptions of the available categories and subcategories. |
| | General Interest-Personal | Select one of the following:<br>• Block<br>• Warn<br>• Allow<br>• Monitor<br>See the FortiGuard web site for descriptions of the available categories and subcategories. |
| | Potentially Liable | Select one of the following:<br>• Block<br>• Warn<br>• Allow<br>• Monitor<br>See the FortiGuard web site for descriptions of the available categories and subcategories. |

| Configuration | | Description |
|---|---|---|
| | Security Risk | Select one of the following:<br>• Block<br>• Warn<br>• Allow<br>• Monitor<br>See the FortiGuard web site for descriptions of the available categories and subcategories. |
| | Unrated | Select one of the following:<br>• Block<br>• Warn<br>• Allow<br>• Monitor<br>See the FortiGuard web site for descriptions of the available categories and subcategories. |
| **Exclusion List** | | |
| Action | | Select one of the following actions:<br>• Block<br>• Allow |
| URL | | Enter specific URLs to block or allow. |
| Type | | Select one of the following types:<br>• Simple<br>• Wildcard<br>• Regular Expression<br>Wildcard characters and Perl Compatible Regular Expressions (PCRE) can be used. |
| **Show Advanced Options** | | Turn on to display and configure basic and advanced options. Turn off to display and configure only basic options. |
| Web Filter | | • Log All URLs<br>• Log user initiated traffic<br>• Enable Safe Search |

## System Settings

| Configuration | Description |
|---|---|
| **Log Settings** | Specify the log settings for FortiClient. |

| Configuration | | Description |
|---|---|---|
| Upload Logs to FortiAnalyzer | | Turn on to upload FortiClient logs to the FortiAnalyzer device at the specified address or hostname. |
| | IP Address | Enter the IP address. |
| | Upload Schedule | Configure the upload schedule in minutes. |
| | Log Retention | Configure the Log Retention in days. |
| | Compress Logs | Enable to compress logs. |

# Log Messages

## Viewing log messages

You can view the log messages generated by FortiClient EMS for Chromebooks.

**To view log messages:**

1. Go to *View* > *View Logs*. The Logs pane is displayed.
2. Click the *Filter* icon in each column heading to apply filters.
3. Click *Clear Filters* to remove the filters.

## Downloading raw logs

You can download the raw logs generated by FortiClient EMS for Chromebooks.

**To download raw logs:**

1. Go to *View* > *View Logs*. The Logs pane is displayed.
2. Click *Raw Logs*.
3. Click the calendar icon in the *Start Date* and *End Date* boxes to select a start date and end date for the logs that you want to download.
4. In the *Levels* box, select one or more levels of logs to include.
5. In the *Sources* list, select one or more sources to include.
6. In the *Message* box, type the log message or messages to include. Leave blank to include all log messages.
   If you want to exclude the log message, enable the *NOT* option.
7. Click the *Calculate Size* button to view the size of the download.
8. Click *Download*.
   A zip of the raw logs is downloaded to your computer.

## Email alert settings

You can add an option to set up an SMTP server to enable an Alert for EMS Events. When an alert is triggered, an email notification will be sent. For more information, see Email alert settings on page 41.

FORTINET®

*High Performance Network Security*